Turyn型Williamson行列について (実験配置の理論と応用)

AUTHOR(S):

山田, 美枝子

CITATION:

山田, 美枝子. Turyn型Williamson行列について (実験配置の理論と応用). 数理解析研究所講究録 1980, 404: 101-116

ISSUE DATE:

1980-11

URL:

http://hdl.handle.net/2433/102312

数理解析研究所講究録
404巻 1980年 101-116

Turyn型 Williamson行列について

東女大 文理 山田美枝子

1. Williamson行列

J. Williamsonは1944年に次のような行列Hを考えた[9].

$$H = \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix},$$

A, B, C, Dはn次対称巡回行列で、成分は+1または-1で

$$A^2 + B^2 + C^2 + D^2 = 4nI \qquad (1)$$

を満足する. ただしIは単位行列. これを4n次Williamson型Hadamard行列あるいは4n次Williamson行列という. すでに4n次Hadamard行列が存在すれば. 2·4n次Hadamard行列を構成することができることが知られているので、nが奇数の場合に、Hadamard行列の存在問題は帰着される. そこで. nを奇数と仮定する.

A, B, C, Dは

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \\ 0 & \cdots\cdots & & 0 & 1 \\ 1 & 0 & \cdots\cdots & & 0 \end{pmatrix}$$

の多項式としてかけるので．T を対角化することにより，(1)式は

$$\left(\sum_{r=0}^{n-1} a_r \zeta_n^r\right)^2 + \left(\sum_{r=0}^{n-1} b_r \zeta_n^r\right)^2 + \left(\sum_{r=0}^{n-1} c_r \zeta_n^r\right)^2 + \left(\sum_{r=0}^{n-1} d_r \zeta_n^r\right)^2 = 4n \qquad (2)$$

と同値になる．a_r, b_r, c_r, d_r $(r=0,\cdots,n-1)$ は A, B, C, D の第1行の成分で，ζ_n は1の n 乗根．ここで $a_0 = b_0 = c_0 = d_0 = 1$ と仮定することができる．さらに

$$a = \sum_{r=0}^{n-1} a_r \zeta_n^r, \quad b = \sum_{r=0}^{n-1} b_r \zeta_n^r, \quad c = \sum_{r=0}^{n-1} c_r \zeta_n^r, \quad d = \sum_{r=0}^{n-1} d_r \zeta_n^r,$$

$$T_1 = \frac{1}{2}(a + b + c - d), \quad T_2 = \frac{1}{2}(a + b - c + d),$$

$$T_3 = \frac{1}{2}(a - b + c + d), \quad T_4 = \frac{1}{2}(-a + b + c + d),$$

とおくと

$$T_1^2 + T_2^2 + T_3^2 + T_4^2 = 4n$$

で，(2)式を

$$\left(1 + 2\sum_{r=1}^{(n-1)/2} e_{r1} u_r\right)^2 + \left(1 + 2\sum_{r=1}^{(n-1)/2} e_{r2} u_r\right)^2 + \left(1 + 2\sum_{r=1}^{(n-1)/2} e_{r3} u_r\right)^2 + \left(1 + 2\sum_{r=1}^{(n-1)/2} e_{r4} u_r\right)^2 = 4n \qquad (3)$$

と変形することができる．このとき $u_r = \zeta_n^r + \zeta_n^{-r}$ $(r=1,\cdots,\frac{n-1}{2})$．$a_0 = b_0 = c_0 = d_0 = 1$ なので，a_r, b_r, c_r, d_r $(r \neq 0)$ のうち3つは同じ符号を持つ[9]ことから，$e_{r1}, e_{r2}, e_{r3}, e_{r4}$ $(r=1,\cdots,\frac{n-1}{2})$ のいずれか1つは $+1$ か -1 で，他の3つは0である．

(2)式または(3)式を Williamson 等式という．Williamson 等式にお

いて $s=1$ とおくと、$4n$ は4つの奇数の平方の和で表わされる。Williamson等式が成りたてばWilliamson行列は存在する。Williamson行列は現在のところ、$n\leq 27$ の奇数についてすべて決定されている[3]。

2. Turyn型 Williamson行列

1972年に R.J. Turyn は Williamson行列に対し、無限系列、ここでいうTuryn型Williamson行列を発見した。すなわち。

定理1 (Turyn, [5]) $q=2n-1$ が素数中 $\equiv 1 \pmod 4$ とすると、$4n$ 次 Williamson 行列が存在する。

Turyn は Paley II 型 Hadamard 行列の有限体の加法群の性質を、Singer 変換により、乗法群の性質におきかえることで、それがWilliamson行列となることを示した。すなわち、Paley II 型 Hadamard 行列の行、列に「入れかえ」や「符号のつけかえ」を行うと、Williamson行列となることを示したのである。その後、1973年にA.L. Whitemanは有限体上2次の拡大体から下の有限体への相対スプールを用いて、この構成が合理化されることを示した。

ここでは有限体上のガウスの和の理論により、整数論的な

構成の意味づけを考える.

3. 有限体上のガウスの和

$F = GF(q)$: q個の元を持つ標数 p の有限体, $q = p^t$,

χ : 単位指標でない F の指標,

S_F : F からの絶対スプール,

$\zeta_p = e^{\frac{2\pi i}{p}}$

とする. F 上のガウスの和 $\tau(\chi)$ は

$$\tau(\chi) = \sum_{\alpha \in F} \chi(\alpha)\, \zeta_p^{S_F \alpha}$$

で定義される. このとき次が成立することが知られている[2].

(1) $\tau(\chi^p) = \tau(\chi)$

(2) $\sigma_\nu : \zeta_p \longrightarrow \zeta_p^\nu$ とするとき, $\sigma_\nu \tau(\chi) = \overline{\chi}(\nu)\, \tau(\chi)$.

(3) $\chi\psi \neq 1$ (単位指標) とするとき, ヤコビの和

$J(\chi, \psi) = -\sum_{\alpha \in F} \chi(\alpha)\psi(1-\alpha)$ は.

$$J(\chi, \psi) = -\frac{\tau(\chi)\cdot\tau(\psi)}{\tau(\chi\psi)}$$

を満足する.

(4) $\chi \neq 1$ とするとき. $\tau(\chi)\cdot\overline{\tau(\chi)} = q$.

(5) Davenport - Hasse の定理.

$q \equiv 1 \pmod m$ なる m について

$$\prod_{\chi^m = 1} \tau(\chi\psi) = -\tau(\psi^m)\psi(m^{-m}) \prod_{\chi^m = 1} \tau(\chi).$$

4. Turyn型 Williamson行列の構成

次の定理が重要である.

定理2 $g = p^t$, $E = GF(g^N)$, $F = GF(g)$

χ: Eの指標でFに制限したとき単位指標でないもの.

$S_{E/F}$: EからFへのスプール. $\tau_E(\chi)$: Eのガウスの和.

$\tau_F(\chi)$: χをFに制限して得られるFのガウスの和とするとき

$\theta_\chi = \dfrac{\tau_E(\chi)}{\tau_F(\chi)}$ とおくと.

$$\theta_\chi = \sum_{S_{E/F}\beta=1} \chi(\beta) = \sum_{\alpha \bmod F^*} \chi(\alpha)\bar{\chi}(S_{E/F}\alpha),$$

で

$$\theta_\chi \cdot \bar{\theta}_\chi = g^{N-1}.$$

(証明) $$\tau_E(\chi) = \sum_{\alpha\in E} \chi(\alpha)\zeta_p^{S_E\alpha} = \sum_{\alpha\in E} \chi(\alpha)\zeta_p^{S_F(S_{E/F}\alpha)}$$

$$= \sum_{a\in F}\sum_{S_{E/F}\alpha=a} \chi(\alpha)\zeta_p^{S_F a} = \sum_{S_{E/F}\alpha=0} \chi(\alpha) + \sum_{a\in F^*}\sum_{S_{E/F}\alpha=a} \chi(\alpha)\zeta_p^{S_F a}.$$

- $S_{E/F}\alpha = a = 0$ のとき $\exists c$, $\chi(c) \neq 1$, $S_{E/F}c\alpha = 0$. そこで
$\sum_{S_{E/F}\alpha=0} \chi(\alpha) = \sum_{S_{E/F}\alpha=0} \chi(c\alpha) = \chi(c)\sum_{S_{E/F}\alpha=0} \chi(\alpha)$. 従って $\sum_{S_{E/F}\alpha=0} \chi(\alpha) = 0$.
- $S_{E/F}\alpha = a \neq 0$ のとき $S_{E/F}\alpha a^{-1} = 1$. そこで $\alpha a^{-1} = \beta$ とおくと. $S_{E/F}\beta = 1$. αは$S_{E/F}\beta = 1$となるβによって$a\beta$の形に一意的に表わされる.

従って

$$\tau_E(\chi) = \sum_{a\in F^*}\sum_{S_{E/F}\beta=1} \chi(a\beta)\zeta_p^{S_F a} = \sum_{a\in F^*} \chi(a)\zeta_p^{S_F a} \cdot \sum_{S_{E/F}\beta=1} \chi(\beta)$$

$$\tau_E(\chi) = \tau_F(\chi) \cdot \sum_{S_{E/F}\beta=1} \chi(\beta).$$

従って

$$\theta_\chi = \frac{\tau_E(\chi)}{\tau_F(\chi)} = \sum_{S_{E/F}\beta=1} \chi(\beta).$$

ところで

$$\chi(\beta) = \chi(\alpha\alpha^{-1}) = \chi(\alpha\cdot(S_{E/F}\alpha)^{-1}) = \chi(\alpha)\cdot\overline{\chi}(S_{E/F}\alpha)$$

で $\chi(\beta)$ の値は α を $c\alpha$, $c\in F^*$ としてもかわらない. なぜなら

$$\chi(c\alpha)\cdot\overline{\chi}(S_{E/F}c\alpha) = \chi(\alpha)\cdot\chi(c)\cdot\overline{\chi}(c)\,\overline{\chi}(S_{E/F}\alpha) = \chi(\alpha)\,\overline{\chi}(S_{E/F}\alpha)$$

であるからである. 代入して次を得る.

$$\theta_\chi = \frac{\tau_E(\chi)}{\tau_F(\chi)} = \sum_{S_{E/F}\beta=1} \chi(\beta) = \sum_{\alpha \bmod^\times F^*} \chi(\alpha)\,\overline{\chi}(S_{E/F}\alpha).$$

また, **3** の (4) より

$$\tau_E(\chi)\cdot\overline{\tau_E(\chi)} = q^N, \qquad \tau_F(\chi)\cdot\overline{\tau_F(\chi)} = q.$$

これより

$$\theta_\chi\cdot\overline{\theta_\chi} = \frac{\tau_E(\chi)}{\tau_F(\chi)}\cdot\frac{\overline{\tau_E(\chi)}}{\overline{\tau_F(\chi)}} = q^{N-1}.$$

Turyn型 Williamson 行列を与えるのは. 上の定理で

$N = 2$, $\quad q \equiv 1 \pmod 4$,

χ を E の指標で F に制限したとき平方剰余指標であるとしたときの θ_χ である. これを示すことで **1** の定理1を証明する.

(定理1の証明)　$q = p^t \equiv 1 \pmod 4$,　$E = GF(q^2)$,

$F = GF(q)$,　ζ_n：1のn乗根,　ξ：Eの生成元,

χ_4：Eの四乗剰余指標,　$\chi_4(\xi) = i$,

χ_n：Eのn乗剰余指標,　$\chi_n(\xi) = \zeta_n$,　χ_nの次数n',　$n' \mid n$,

$\chi = \chi_4 \cdot \chi_n$：$E$の指標で$F$に制限したとき平方剰余指標となる、として上の定理2を考えると.

$$\theta_\chi = \frac{\tau_E(\chi)}{\tau_F(\chi)} = \sum_{r=0}^{q} \chi_4(\xi^r)\chi_n(\xi^r)\chi(S_{E/F}\xi^r) = \sum_{r=0}^{q} (i)^r(\zeta_n)^r \chi(S_{E/F}\xi^r),$$

rを偶数、奇数にわけると.

$$\theta_\chi = \sum_{r=0}^{n-1} \{ i^{2r}\zeta_n^{2r}\chi(S_{E/F}\xi^{2r}) + i^{2r+n}\zeta_n^{2r+n}\chi(S_{E/F}\xi^{2r+n}) \}$$

$$= \sum_{r=0}^{n-1} (-1)^r \{ \chi(S_{E/F}\xi^{2r}) + i^n \chi(S_{E/F}\xi^{2r+n}) \} \zeta_n^{2r}.$$

ここで

$$\beta_r = \frac{(-1)^{\frac{n+1}{2}+r}}{-1+i} \{ \chi(S_{E/F}\xi^{2r}) + i^n \chi(S_{E/F}\xi^{2r+n}) \} \quad (r=0, \cdots, n-1)$$

とおくと、β_0は$\psi(2) = (-1)^{\frac{n-1}{2}}$より

$$\beta_0 = \frac{(-1)^{\frac{n+1}{2}}}{-1+i}\psi(2) = \frac{(-1)^{\frac{n+1}{2}}(-1)^{\frac{n-1}{2}}}{-1+i} = \frac{1+i}{2},$$

その他のβ_r ($r=1, \cdots, n-1$)は± 1または$\pm i$のいずれかで、$\beta_{n-r} = \beta_r$である.　θ_χを次のように変形する.

$$\theta_\chi = (-1)^{\frac{n+1}{2}}(-1+i)\left\{\frac{1+i}{2} + \sum_{r=1}^{n-1}\beta_r \zeta_n^{2r}\right\} = (-1)^{\frac{n+1}{2}}(-1+i)K_\chi.$$

定理2から、$\theta_\chi \cdot \overline{\theta_\chi} = g$。$2K_\chi \cdot 2\overline{K_\chi} = 2g$。従って

$$2 + 2K_\chi \cdot 2\overline{K_\chi} = 1^2 + 1^2 + \left(1 + 2\sum_{r\in A_+} u_r - 2\sum_{r\in A_-} u_r\right)^2 + \left(1 + 2\sum_{r\in B_+} u_r - 2\sum_{r\in B_-} u_r\right)^2$$

$$= 2 + 2g = 2(1+g) = 4n,$$

A_+, A_-, B_+, B_- は β_r が $1, -1, i, -i$ によって $\Omega = \{1, \cdots, \frac{n-1}{2}\}$ を4分割した部分集合である。

Williamson 等式が成立したので Williamson行列は存在する。

5. Toryn型 Williamson 行列を与えるガウスの和の比 θ_χ の考察

Toryn型 Williamson 行列を与えるのは、**4** によって $E = GF(g^2)$ のガウスの和 $\zeta_E(\chi)$ と $F = GF(g)$ のガウスの和 $\zeta_F(\chi)$ の比 θ_χ であることがわかった。Paley II型 Hadamard 行列で無限遠点を除いた行列を生成するのは、有限体上のガウスの和であった。行、列の「入れかえ」,「符号のつけかえ」を行うことで得られる Toryn型 Williamson 行列が、無限遠点を含んだ乗法群として考えると、Paley II型とは異なる θ_χ によって得られるのは大変不思議なことである。

そこで、この θ_χ について考察する。

有限体上のガウスの和と、その拡大体のガウスの和との関

係について．次の定理がある．

定理3 （Davenport - Hasse の定理，[2]） $q = p^t$，$E = GF(q^N)$，$F = GF(q)$，χ_E：E の指標，χ_F：F の指標，$N_{E/F}$：E から F へのノルム，$\chi_E = \chi_F \cdot N_{E/F}$ とすると．

$$-\tau(\chi_E) = \left(-\tau(\chi_F)\right)^N.$$

この定理により．次の定理が導かれる．

定理4 Turyn型 Williamson 行列を与える θ_χ は

$$\theta_\chi^2 = \left(\frac{\tau_E(\chi)}{\tau_F(\chi)}\right)^2 = J(\chi, \chi^q)$$

を満足する．

（証明）
$$-\tau_E(\chi^{1+q}) = \frac{-\tau_E(\chi)\cdot\tau_E(\chi^q)}{-J(\chi,\chi^q)} - \frac{\tau_E(\chi)^2}{J(\chi,\chi^q)}.$$

一方、E の生成元 ξ に対し．

$$\chi^{1+q}(\xi) = \chi(\xi^{1+q}) = \chi(N_{E/F}\xi).$$

Davenport - Hasse の定理より

$$\tau_E(\chi^{1+q}) = \left(-\tau_F(\chi)\right)^2 = \tau_F(\chi)^2$$

を得る．最初の式に代入して．$\theta^2 = J(\chi,\chi^q)$ が求まる．

$\mathbb{Q}_4$自身が何であるか知るために、円周$4n$等分体での素イデアル分解を求める。準備として、有限体のTeichmüller指標を定義する。

<u>定義</u>　$q=p^t$,　$\mathcal{O}$：円周$q-1$等分体$\mathbb{Q}(\zeta_{q-1})$の整数環,　$F=GF(q)$,　ξ_{q-1}：Fの生成元,　ζ_{q-1}：1の原始$q-1$乗根とする。$\mathcal{O}$のpをわるある素イデアル$\mathfrak{p}$に対し、$\mathcal{O}/\mathfrak{p}$とF^*を同一にみなすことができる。すなわち$\mathfrak{p}$の原始根がζ_{q-1}にとれて

$$\varphi(\zeta_{q-1})=\zeta_{q-1}$$

なる同型対応φが存在する。そこで、ωを$\mathcal{O}/\mathfrak{p}$の指標で$\omega(\zeta_{q-1})=\zeta_{q-1}$とするとき、$\xi_{q-1}\in F^*$に対し、

$$\omega(\xi_{q-1})=\omega(\varphi(\xi_{q-1}))=\omega(\zeta_{q-1})=\zeta_{q-1}$$

として、F^*の指標ωを定義する。これを$\mathfrak{p}$に対する<u>Teichmüller指標</u>とよぶ[2]。

このTeichmüller指標ωは、F^*の指標をすべて生成する。F^*の任意の指標χはωの中である。

ガウスの和の素イデアル分解を与える次の定理がある。

定理5 (Stickelberger の定理, [2]) $q=p^f$,

ω: 円周 $q-1$ 等分体 $Q(\zeta_{q-1})$ の p をわる素イデアル $\mathfrak{P}$ に対する Teichmüller 指標,

ω^{-k}: m 次の $F=GF(q)$ の指標,

$\mathfrak{p}$: 円周 m 等分体 $Q(\zeta_m)$ の p をわる素イデアル,

f : $p^f \equiv 1 \pmod m$ となる最小の f,

$Z^*(m)$: $\bmod m$ の既約剰余類,

$\langle a \rangle$: a の小数部分を示す,

σ_c : $Q(\zeta_m)$ の自己同型写像, $\zeta_m \to \zeta_m^c$,

N: $Q(\zeta_{q-1})$ から $Q(\zeta_m)$ へのノルム,

$\theta(k,\mathfrak{p}) = \sum_{c\in Z^*(m)} \left\langle \frac{kc}{q-1} \right\rangle \sigma_c^{-1}$: Stickelberger element,

とする. 円周 m 等分体 $Q(\zeta_m)$ でのガウスの和 $\tau(\omega^{-k})$ の素イデアル分解は次で与えられる.

$$\tau(\omega^{-k}) \sim \mathfrak{p}^{\frac{t}{f}\theta(k,\mathfrak{p})} \sim \mathfrak{p}^{\frac{t}{f}\sum_{c\in Z^*(m)}\left\langle \frac{kc}{q-1}\right\rangle \sigma_c^{-1}} \sim N(\mathfrak{P})^{\theta(k,\mathfrak{p})}.$$

この定理から. θ_x の素イデアル分解を求める.

定理6 Turyn 型 Williamson 行列を与える θ_x の素イデアル分解は次で与えられる.

$$\theta_\chi \sim \mathfrak{P}^{\theta}, \quad \theta = \frac{t}{f} \sum_{c \in \mathbb{Z}^*(4n'),\, B_1(\langle -\frac{c}{4} - \frac{c}{n'} \rangle) > 0} \sigma_c^{-1},$$

ただし、 $\mathfrak{P}$ ：円周 $4n'$ 等分体 $\mathbb{Q}(\zeta_{4n'})$ での p をわる素イデアル，

f ： $p^f \equiv 1 \pmod{4n'}$ となる最小の f，

$\mathbb{Z}^*(4n')$ ： $\bmod 4n'$ の既約剰余類，

$B_1(x) = x - \frac{1}{2}$ ：一次のベルヌイ多項式

σ_c ： $\mathbb{Q}(\zeta_{4n'})$ の自己同型写像， $\zeta_{4n'} \to \zeta_{4n'}^{c}$.

(証明) χ は円周 g^2-1 等分体 $\mathbb{Q}(\zeta_{g^2-1})$ の p をわる素イデアル $\mathfrak{p}$ に対する Teichmüller 指標に関して

$$\chi = \omega^{\frac{g^2-1}{4} + \frac{g^2-1}{n'}}$$

とかける．Stickelberger の定理により．$\mathfrak{p} | \mathfrak{P}$ なる素イデアル $\mathfrak{P}$ について

$$\tau_E(\chi) \sim \mathfrak{P}^{\frac{2t}{f}\theta(k,\mathfrak{P})} \sim \mathfrak{P}^{\frac{2t}{f}\sum_{c \in \mathbb{Z}^*(4n')} \langle -\frac{c}{4} - \frac{c}{n'} \rangle \sigma_c^{-1}}.$$

χ を F に制限すると，円周 $g-1$ 等分体の $\mathfrak{p}$ でわれる素イデアルに対し，同じ Teichmüller 指標がとれて．

$$\chi = \chi_F = \omega^{\frac{g-1}{2}}$$

とかける．そこで

$$\tau_F(\chi) \sim p^{\frac{t}{2}}.$$

素数 p は．$\mathbb{Q}(\zeta_{4n'})$ で分解するので．$\tau_F(\chi)$ は $\mathbb{Q}(\zeta_{4n'})$ で次のように素イデアル分解される．

$$\tau_{F_1}(\chi) \sim p^{\frac{t}{2}} \sim \mathfrak{p}^{\frac{t}{2}\cdot\frac{1}{f}\sum_{c\in\mathbb{Z}^*(4n')}\sigma_c^{-1}} \sim \mathfrak{p}^{\frac{t}{f}\sum_{c\in\mathbb{Z}^*(4n')}\frac{1}{2}\sigma_c^{-1}}.$$

従って、θ_χ の $Q(\zeta_{4n'})$ での素イデアル分解は

$$\theta_\chi = \frac{\tau_E(\chi)}{\tau_{F_1}(\chi)} \sim \mathfrak{p}^{\frac{t}{f}\left\{\sum_{c\in\mathbb{Z}^*(4n')}\left(2\langle -\frac{c}{4}-\frac{c}{n'}\rangle-\frac{1}{2}\right)\sigma_c^{-1}\right\}} \sim \mathfrak{p}^{\theta}.$$

$\mathfrak{p}$ の肩の部分 θ を簡約する。各 c に対し次が成立する。

$$\begin{aligned}\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle &= \left\langle -\frac{c(2n-1)}{4}-\frac{c(2n-1)}{n'}\right\rangle = \left\langle -\frac{c}{4}+\frac{c}{n'}\right\rangle \\ &= \left\langle -\frac{c}{2}+\frac{c}{4}+\frac{c}{n'}\right\rangle = \left\langle \frac{1}{2}-\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right\rangle \\ &= \left\langle -B_1\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right)\right\rangle.\end{aligned}$$

そこで

- $B_1\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right) > 0$ のとき

$$\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle = 1 - B_1\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right) = \frac{3}{2}-\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle,$$

$$B_1\left(\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle\right) > 0.$$

- $B_1\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right) \leqq 0$ のとき

$$\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle = -B_1\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\right) = \frac{1}{2}-\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle,$$

$$B_1\left(\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle\right) \leqq 0.$$

このことから

$$\begin{aligned}\theta &= \frac{t}{f}\left\{\sum_{c\in\mathbb{Z}^*(4n')}\left(2\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle-\frac{1}{2}\right)\sigma_c^{-1}\right\} \\ &= \frac{t}{f}\left\{\sum_{c\in\mathbb{Z}^*(4n')}\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle\sigma_c^{-1}+\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle\sigma_{c\mathfrak{g}}^{-1}-\frac{1}{2}\sigma_c^{-1}\right\} \\ &= \frac{t}{f}\left\{\sum_{c\in\mathbb{Z}^*(4n')}\left(\left\langle -\frac{c}{4}-\frac{c}{n'}\right\rangle+\left\langle -\frac{c\mathfrak{g}}{4}-\frac{c\mathfrak{g}}{n'}\right\rangle\right)\sigma_c^{-1}-\frac{1}{2}\sigma_c^{-1}\right\}\end{aligned}$$

$$= \frac{t}{f}\left\{ \sum_{B_1(\langle -\frac{c}{4}-\frac{c}{n'}\rangle)>0} \frac{3}{2}\sigma_c^{-1} + \sum_{B_1(\langle -\frac{c}{4}-\frac{c}{n'}\rangle)\leq 0} \frac{1}{2}\sigma_c^{-1} - \sum_{c\in\mathbb{Z}^*(4n')} \frac{1}{2}\sigma_c^{-1} \right\}$$

$$= \frac{t}{f} \sum_{B_1(\langle -\frac{c}{4}-\frac{c}{n'}\rangle)>0} \sigma_c^{-1}.$$

今、特に $n'=1$, すなわち $\chi=\chi_4$ とおくと、

$$\theta_x \sim g^{\theta}, \quad \theta = \begin{cases} t\sigma_1 & (p\equiv 1 \pmod 4) \\ \frac{t}{2}\sigma_1 & (p\equiv 3 \pmod 4) \end{cases}$$

を得る。ノルムをとることで、g を2つの奇数の平方の和に分ける表わし方が決定される。それと、沢出の結果[4]から A_+, A_-, B_+, B_- の濃度を決定することができる。また、このことは Turyn型 Williamson行列より生成される Supplementary difference sets [8] のそれを構成する各集合の濃度が決定されることも意味するのである。

6. 今後の課題

Turyn型 Williamson行列を生成するものが、θ_x、すなわちガウスの和の比と解釈したが、もっと自然な解釈が存在するかもしれない。しかし、それはまだ解決されていない。具体的な値を与えて、いくつか θ_x を求め分布を調べたが、規則性等何のアイデアも今のところ得ていない。この構成を発展させて新しい Williamson行列が得られるかどうかということも、今後

に残された大きな課題である.

参考文献

1. H. Hasse, Vorlesungen über Zahlentheorie, Springer, Berlin, 1964.
2. S. Lang, Cyclotomic Fields, Springer, New York, 1978.
3. K. Sawade, Hadamard matrices of order 100 and 108, Bull. of Nagoya Institute of Technology 29 (1977), 147-153.
4. 沢出和江, ある特殊なWilliamson等式, 京都大学数理解析研究所講究録, 本号.
5. R.J. Turyn, An infinite class of Williamson matrices, J. Combinatorial Theory, Ser. A 12 (1972), 319-321.
6. W.D. Wallis, A.P. Street and J.S. Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Math.,vol. 292, Springer, New York, 1972.
7. A.L. Whiteman, An infinite family of Hadamard matrices of Williamson type, J. Combinatorial Theory, Ser. A 14 (1973), 334-340.
8. A.L. Whiteman, Hadamard matrices of order 4(2p+1), J. Number Theory 8 (1976), 1-11.
9. J. Williamson, Hadamard's determinant theorem and sum of four squares, Duke Math. J. 11 (1944), 65-81.
10. M. Yamada, On the Williamson type j matrices of orders 4•29, 4•41, and 4•37, J. Combinatorial Theory, Ser. A 27 (1979), 378-381.

11. 山本幸一，Williamson型 Hadamard 行列と Shift register 列について，大阪市立大学での研究集会「実験計画法とその関連分野」の予稿集，1978 年12月．